REMARKS

Applicants respectfully request reconsideration of the present Application in view of the foregoing amendments and in view of the reasons that follow.

With this Amendment, Claims 1, 14 and 19 have been amended. No Claims have been canceled or newly added. A detailed listing of all claims that are, or were, in the Application, irrespective of whether the claims remain under examination in the Application, is presented, with appropriately defined status identifiers. Thus, Claims 1-20 remain pending in the Application.

Support for the amendments to Claims 1, 14 and 19 can be found in the disclosure in at least the following: paragraph [00026]. No new matter has been added.

Claim Rejections - 35 USC § 103

Claims 1-6 and 13-15 were rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Publication No. 2003/0171112 to Lupper, et al. (Lupper), in view of U.S. Patent 6,715,082 to Chang, et al. (Chang), and further in view of U.S. Patent No. 5,398,285 to Borgelt, et al. (Borgelt), and further in view of U.S. Patent No. 6,470,454 to Challener (Challener). Claims 7-11, 16 and 18 were rejected under 35 U.S.C. §103(a) as being unpatentable over Lupper, in view of Chang, in view of Borgelt, and in further view of U.S. Patent No. 6,463,055 to Lupien, et al. (Lupien). Claim 17 was rejected under 35 U.S.C. §103(a) as being unpatentable over Lupper, in view of Chang, in view of Borgelt, and in further view of U.S. Publication No. 2003/0051041 to Kalavade, et al. (Kalavade). Claims 19 and 20 were rejected under 35 U.S.C. §103(a) as being unpatentable over Lupper, in view of Chang, in view of Lupien, in view of Borgelt, in view of Challener, and further in view of Kalavade. Applicants respectfully request withdrawal of the rejection.

As an initial matter, independent claims 1 and 14 where rejected by the combination of references listed above, **including** Challener. However, in rejecting dependent claims 7-11, 16 and 18, which depend respectively from claims 1 and 14, the

combination of references does **not** include Challener. This does not seem proper. Thus, for the record, Applicants respectfully request clarification for the rejection of claims 7-11, 16 and 18.

To establish *prima facie* obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). *See also* MPEP 2143.03. Independent claims 1, 14, and 19 have been amended merely to clarify what is being claimed, and in no way has been amended to overcome the present rejection. Applicants respectfully submit that the claims presented in the Amendment dated July 7, 2009 are clearly not disclosed, taught or otherwise rendered obvious over the combination of Lupper, Chang, Borgelt and Challener. In particular, claim 1 has been amended to recite "creating a one-time entropy generated password for a client including: calculating a hash value based on an identification information of the client, an encryption key provided by the WPAN, and a predetermined text character string, wherein the calculated hash value includes a plurality of octet values; and subsequently converting any non-alphanumeric octet values of the plurality of octet values of the calculated hash value into an alphanumeric octet value." Independent claims 14 and 19 have been similarly amended. This feature is neither taught nor suggest by Lupper, Chang, Borgelt, Lupien, Challener, Kalavade, or any combination thereof.

The Office Action alleges that "Lupper discloses a generic WLAN architecture wherein a subscriber name and password are obtained from the subscriber and compared to locally available subscriber data records (citing paragraph [0078] of Lupper), which meets the limitation of creating a password for a client." Office Action, page 3. Applicants respectfully disagree.

Lupper states at paragraph [0078]:

> The subscriber identification data (name, password) ***obtained*** from the subscriber or subscriber terminal W-H can now be verified by the data selection server SSG by either accessing locally available subscriber data records

> (AAA server) or subscriber data records in other local networks (AAA client) or subscriber data records in second, heterogeneous networks GSM, UMTS, PSTN. (emphasis added).

In other words, Lupper does not ***create*** a password, let alone create a password by calculating a hash value and subsequently converting any non-alphanumeric octet values of the plurality of octet values of the calculated hash value into an alphanumeric octet value, as claimed, but merely ***obtains*** subscriber identification data. Moreover, the subscriber identification data obtained from the subscriber is not a password, whereby a client with a smart card is enabled to utilize a public wireless local area network (WPAN).

The Office Action concedes that:

> Lupper and Chang do not specify passwords that are generated using an identifier, encryption key, and a character string. Borgelt discloses passwords generated utilizing an identifier (citing, Figure 2, 200), encryption key (citing, Figure 2, 202), and a software code (citing Figure 2, 201). It would have been obvious to one of ordinary skill in the art at the time of the invention was made to generate the passwords of Lupper, as modified with Chang, with an identifier, key, and additional character string, in order to utilize passwords that are unique to users and not easily obtainable as taught by Borgelt (citing, column 2, lines 7-11)." Office Action, pages 3-4.

Applicants respectfully disagree. First, as discussed above, Lupper does not disclose, teach or otherwise render obvious the recited creation of a password.

Moreover, as recited in claim 1, the recited one-time entropy generated password for a client includes ***calculating a hash value based on an identification information of the client, an encryption key provided by the WPAN, and a predetermined text character string***. In contrast, Borgelt discloses that a hardware ID and embedded software code from either base station 101 or communication unit 102 are combined into a single code and then this single code is encrypted by a system controller 103

using a private encryption key that is kept private (i.e., does not leave the factory or system controller 103). *See*, lines 28-30 and 44-54 of column 4 of Borgelt. In other words, Borgelt uses two pieces of data, the hardware ID and the embedded software code, and encrypts this data with a private key to create a password. The private key of Borgelt is used not as an input to the password creation process, as claimed, but is a mechanism that is used to create password from the hardware ID and the embedded software code.

Further, as discussed above, the private key of Borgelt is not provided by the WPAN, as claimed, but is stored in the system controller 103.

The Office Action concedes that:

> Lupper, Change, and Borgelt do not disclose hashing the calculation to generate the password by converting non-alphanumerics to alphanumerics. Challener discloses generating passwords by calculating a hash value and converting all non-alphanumerics to alphanumerics (citing, Col. 4, line 24 & Col. 5, lines 10-15), which meets the limitation of creating comprises calculating a hash value using SHA-1 hashing process, comprising a plurality of octet values and subsequently converting any non-alphanumeric octet values of the plurality of octet values of the hash value into an alphanumeric octet value." Office Action, page 4.

Applicants respectfully disagree. First, the cited portions of Challener do not disclose, teach or otherwise render obvious at least the features of "creating a one-time entropy generated password for a client including ***calculating a hash value*** based on an ***identification information of the client***, ***an encryption key provided by the WPAN***, and a ***predetermined text character string***, wherein the calculated hash value includes a plurality of octet values; and ***subsequently converting*** any non-alphanumeric octet values of the plurality of octet values of the calculated hash value into an alphanumeric octet value."

Moreover, there would be no motivation to combine Challener with the alleged Lupper, Chang, Borgelt combination. As discussed above, Borgelt creates a password by encrypting a combination of the hardware ID and embedded software code with a

private key stored in the system controller 103. This encrypted password is transferred to the communication device 102 and is then decrypted using a public decryption key. *See*, lines 66-68 of column 4 of Borgelt. One of ordinary skill in the art would not have used the hashing function of Challener on Borgelt's encrypted password, as alleged in the Office Action, since the communication device 102 could not have successfully performed a password decryption using the public decryption key if the encrypted password had been subjected to a further hashing operation. Since the proposed modification of the alleged Lupper, Chang, Borgelt combination with the teachings of Challener would render at least Borgelt unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification. *See*, MPEP 2143.01 V citing *In re Gordon*, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984).

The additions of Chang, Borgelt, Challener, Lupien, Challener, or Kalavade, do not cure the above-noted deficiencies of Lupper. Moreover, beyond the fact that the cited portions of Lupper, Borgelt, Challener, Lupien, Challener, or Kalavade, fail to teach the claimed invention, the Office Action has not established the requisite and proper analysis as to how and why one of ordinary skill in the art would combine and/or modify Lupper, Borgelt, Challener, Lupien, Challener, or Kalavade to arrive at the claimed invention. *See KSR Int'l. Co. v. Teleflex, Inc.*, 127 S. Ct. 1727, 1741 (2007) (a determination, with supporting evidence, must be made as to "whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue. To facilitate review, this analysis should be made explicit"). Instead, the Office Action merely offers the conclusory statements above. This is clearly inadequate under the Supreme Court's *KSR* decision since the Office Action cites nothing which supports such a conclusion.

In fact, persons of ordinary skill in this art would recognize that Lupper, Borgelt, Challener, Lupien, Challener, or Kalavade are not properly combinable for at least the reasons provided above and the fact that neither Lupper, Borgelt, Challener, Lupien, Challener, or Kalavade disclose, teach or otherwise render obvious at least the recited features of "***creating a one-time entropy generated password*** for a client including

calculating a hash value based on an ***identification information of the client***, ***an encryption key provided by the WPAN***, and a ***predetermined text character string***, wherein the calculated hash value includes a plurality of octet values; and ***subsequently converting*** any non-alphanumeric octet values of the plurality of octet values of the calculated hash value into an alphanumeric octet value," as recited in claim 1. Independent claims 14 and 19 recite similar features. The Examiner has, at best, used Applicants own disclosure as a roadmap to combine and modify Lupper, Borgelt, Challener, Lupien, Challener, or Kalavade to arrive at the clamed invention. Applicants submit that the Examiner is simply engaging in hindsight reasoning, which has been long held to be improper. As such, the Office Action's rationale for modifying Lupper is merely speculative.

Thus, Applicants respectfully submit that neither Lupper, Borgelt, Challener, Lupien, Challener, or Kalavade, either individually or in combination, disclose, teach or otherwise render obvious all the features recited in claim 1. Therefore, claim 1 should be allowable at least for this reason. Independent claims 14 and 19 recite a system and method, respectively, with features similar to claim 1, should be allowable at least for the same reason. Dependent claims 2-11, 13, 15-18 and 20 depend upon base independent claims 1, 14 or 19, and should be allowable by reason of their dependency upon an allowable base claim.

CONCLUSION

Consequently, in view of the foregoing amendment and remarks, it is respectfully submitted that the present Application, including Claims 1-20, is patently distinguished over the prior art, in condition for allowance, and such action is respectfully requested at an early date.

In view of the above amendment, applicant believes the pending application is in condition for allowance. The Director is authorized to charge any fees necessary and/or credit any overpayments to Deposit Account No. 03-3975, referencing Docket No. 043395-0378353.

Respectfully submitted,

Dated: December 28, 2009 By:

/Christopher M. Tucker/

Christopher M. Tucker
Registration No. 48,783
Attorney for Applicant(s)

Customer No. 00909
PILLSBURY WINTHROP SHAW PITTMAN LLP
P.O. Box 10500
McLean, VA 22102
Telephone: 703-770-7900
Facsimile: 703-770-7901